Отчет о пентесте

Общая информация о тестировании:
Отчет содержит результаты проведенных работ по проверке наличия уязвимостей внешнего периметра (далее – Система) компании АО «XXXX», выполненных в соответствии с договором от _____ г. № XXXX, заключенным между Исполнителем и АО «XXX». В отчете содержится описание выявленных недостатков и связанных с ними уровней критичности.
Объект тестирования: сайт <название>
Тестирование провел: Колесников С. В.
Методика проведения тестирования:

1) сканирование на инъекции
2) проверка безопасности авторизации
3) сканирование на известные уязвимости

Дата: 12.07.2024

Обнаруженные уязвимости:

Название	Описание	Риск cvssv3/cvssv2	Ссылка
CVE-2013-1824	SOAP-парсер в PHP до версии 5.3.22 и 5.4.x до версии 5.4.12 позволяет удаленным злоумышленникам читать произвольные файлы через SOAP WSDL-файл, содержащий внешнее объявление XML-сущности в сочетании с ссылкой на сущность, связанную с проблемой XML External Entity (XXE) в функциях soap_xmlParseFile и soap_xmlParseMemory.	4.3 Medium	https://nvd.nist.gov/vuln/detail/CVE-2013-1824
CVE-2013-4113	ext/xml/xml.c в PHP до версии 5.3.27 неправильно учитывает глубину разбора, что позволяет удаленным злоумышленникам вызывать отказ в обслуживании (повреждение кучи памяти) или может иметь другое неопределенное влияние через специально созданный документ, который	6.8 Medium	https://nvd.nist.gov/vuln/detail/CVE-2013-4113

	обрабатывается функцией xml_parse_into_struct.		
CVE-2013-2110	Переполнение буфера на основе кучи в функции php_quot_print_encode в ext/standard/quot_print.c в PHP до версии 5.3.26 и 5.4.x до версии 5.4.16 позволяет удаленным злоумышленникам вызывать отказ в обслуживании (падение приложения) или может иметь другое неопределенное влияние через специально созданный аргумент к функции quoted_printable_encode.	5.0 Medium	https://nvd.nist.gov/vuln/detail/CVE-2013-2110
CVE-2013-4635	Переполнение значения целого числа в функции SdnToJewish в jewish.c в компоненте календаря в PHP до версии 5.3.26 и 5.4.x до версии 5.4.16 позволяет злоумышленникам в зависимости от контекста вызывать отказ в обслуживании (зависание приложения) через большое значение аргумента к функции jdtojewish.	5.0 Medium	https://nvd.nist.gov/vuln/detail/CVE-2013-4635

Описание проделанной работы:
Проводилось сканирование с использованием инструмента Metasploit Framework.

Подробный технический отчет:
Отчет Metasploit Framework расположен по ссылке.